Des. Codes Cryptogr. (2017) 84:415–424
DOI 10.1007/s10623-016-0275-7

Near-complete external difference families

James A. Davis[1] · **Sophie Huczynska**[2] ·
Gary L. Mullen[3]

Received: 6 February 2016 / Revised: 3 August 2016 / Accepted: 19 August 2016 /
Published online: 30 August 2016

Abstract We introduce and explore *near-complete external difference families*, a partitioning of the nonidentity elements of a group so that each nonidentity element is expressible as a difference of elements from distinct subsets a fixed number of times. We show that the existence of such an object implies the existence of a near-resolvable design. We provide examples and general constructions of these objects, some of which lead to new parameter families of near-resolvable designs on a non-prime-power number of points. Our constructions employ cyclotomy, partial difference sets, and Galois rings.

Keywords Difference family · Galois rings · Partial difference sets

Mathematics Subject Classification 94C30 · 51E20 · 94A62 · 05B10

1 Introduction

Difference families (DFs) of various types have long been studied in combinatorial literature, and they have been used to construct combinatorial objects such as designs and strongly

Communicated by D. Jungnickel.

✉ James A. Davis
jdavis@richmond.edu

Sophie Huczynska
Sophie.Huczynska@st-andrews.ac.uk

Gary L. Mullen
mullen@math.psu.edu

1 Department of Mathematics and Computer Science, University of Richmond, Richmond, VA 23173, USA

2 School of Mathematics and Statistics, University of St. Andrews, St. Andrews, Fife KY16 9SS, Scotland, UK

3 Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

regular graphs (see [1,7,17]). In a DF of sets, each nonidentity element of a group will arise some fixed number of times as a difference between same-set elements. External DFs (EDFs) were introduced in [14] as a method of constructing optimal robust secret sharing schemes. In an EDF, as the name suggests, each nonidentity element arises a fixed number of times as a difference between elements in *distinct* sets. Chang and Ding [2] recognized that EDFs have a connection with difference systems of sets (DSSs), first introduced by Levenshtein [9], a combinatorial configuration that arises in connection with code synchronization (see [5,12]); specifically, EDFs generalize *perfect*, *regular* DSSs. In this paper, we will focus on those EDFs whose sets partition the nonidentity elements of a group, which we call *near-complete* EDFs. Ng and Paterson [13] have recently written a survey on disjoint DFs (DDFs), and the near-complete EDFs introduced in this paper will also be near-complete DDFs. For all these reasons, we claim that near-complete EDFs are natural objects to study with a particularly nice structure, and we support this claim by highlighting their connections with other combinatorial objects.

2 Motivation: multiplicative cosets in finite fields

Our initial motivation arose from the following observation about the cosets of a multiplicative subgroup in a finite field (see [10] or [11] for background on finite fields). If q is a prime power, then the multiplicative group of the finite field $GF(q)$ is cyclic: we denote the multiplicative group by $GF(q)^*$. If H is a multiplicative subgroup then there will be $\frac{q-1}{|H|}$ cosets of H in $GF(q)^*$ where, as usual, $|H|$ denotes the number of elements in H.

Theorem 2.1 *Let H be a multiplicative subgroup of a field $GF(q)$ and let $\{D_1, D_2, \ldots, D_{(q-1)/|H|}\}$ be the cosets of H in $GF(q)^*$. If $x \in GF(q)^*$, then $x = g - g'$ for $q - 1 - |H|$ elements $(g, g') \in \cup_{i \neq j} D_i \times D_j$.*

Proof We include the proof for reference later in the paper: a version of this result was originally proved in [18]. Let $x, y \in GF(q)^*$, $x \neq y$ and suppose $x = g - g'$ for $g \in D_i$, $g' \in D_j$, $1 \leq i \neq j \leq (q-1)/|H|$. There is a $z \in GF(q)^*$ so that $y = zx$ and hence we get the equation $y = zg - zg'$. We see that zg and zg' are in distinct multiplicative cosets of H, so we have produced a solution to the difference equation for y. We can reverse this process to show that every difference for y will also produce a difference for x and therefore every element of $GF(q)^*$ will have the same number of differences. There are

$$\frac{q-1}{|H|}\left(\frac{q-1}{|H|} - 1\right)|H|^2,$$

elements of $\cup_{i \neq j} D_i \times D_j$, and each of these will produce a difference in $GF(q)^*$, so each $x \in GF(q)^*$ will have

$$\frac{\frac{q-1}{|H|}\left(\frac{q-1}{|H|} - 1\right)|H|^2}{q-1} = q - 1 - |H|,$$

differences $x = g - g'$ for $(g, g') \in \cup_{i \neq j} D_i \times D_j$. □

Motivated by this example, we are ready to define the main objects of study in this paper. We will state our definitions and many of our results for general groups G, but we will use the binary operation of addition unless otherwise stated. We are following the notation of [2].

Definition 2.2 Let G be a finite group of order v and let $D_1, D_2, \ldots, D_u$ be subsets of G of order k that are mutually disjoint. We say that $\{D_1, D_2, \ldots, D_u\}$ is a $(v, k, \lambda; u)$ EDF in G if every nonidentity element $x \in G$ has λ differences $x = g - g'$ where $g \in D_i$, $g' \in D_j$, $i \neq j$. If $\{D_1, D_2, \ldots, D_u\}$ partitions the nonidentity elements of G, then we say that $\{D_1, D_2, \ldots, D_u\}$ is a $(v, k, \lambda; u)$ near-complete EDF in G.

Theorem 2.1 implies that $\{D_1, D_2, \ldots, D_{q-1/|H|}\}$, the set of multiplicative cosets of H in $GF(q)$, forms a $\left(q, |H|, q-1-|H|; \frac{q-1}{|H|}\right)$ near-complete EDF in the additive group of $GF(q)$. If we have a $(v, k, \lambda; u)$ near-complete EDF, then $v = ku + 1$ and $(v-1)\lambda = u(u-1)k^2$, i.e., $\lambda = k(u-1)$. Thus, we can write the parameters of the near-complete EDF as $(ku+1, k, k(u-1); u)$.

For the construction of Theorem 2.1, observe that the full set of differences $g - g'$, where $g, g' \in GF(q)^*$, contains each element of $GF(q)^*$ precisely $q-2$ times. Hence, each element of $GF(q)^*$ occurs a fixed number of times as a difference within cosets, namely $|H| - 1$ times. This implies a connection with traditional DFs. We recap the definition here, focussing on a particular type which will be important for us.

Definition 2.3 Let G be a finite group of order v and let $D_1, D_2, \ldots, D_u$ be k-subsets of G. We say that $\{D_1, D_2, \ldots, D_u\}$ is a $(v, k, \lambda; u)$ DF in G if every nonidentity element $x \in G$ has λ differences $x = g - g'$, where $g, g' \in D_i$ for some i. If $u = 1$, we call this a difference set (DS). If the D_i are a DF and are mutually disjoint then we say that $\{D_1, D_2, \ldots, D_u\}$ is a $(v, k, \lambda; u)$ DDF in G. If the D_i partition the nonidentity elements of G, then we say that $\{D_1, D_2, \ldots, D_u\}$ is a $(v, k, \lambda; u)$ near-complete DDF.

It transpires that the above observation about Theorem 2.1 is an example of a general result; namely that a near-complete EDF in a group G is precisely a near-complete DDF. This follows from analogous reasoning to the above: each nonidentity element of G occurs $|G^*| - 1$ times as a difference from pairs in $G^* \times G^*$, and so if each element occurs the same fixed number of times as an internal difference, it also occurs a fixed number of times as an external difference, and vice versa. A formal proof of this result can be found in Proposition 2 in [2].

Theorem 2.4 *The collection of subsets* $\{D_1, D_2, \ldots, D_u\}$ *of a group* G *forms a* $(ku+1, k, k(u-1); u)$ *near-complete EDF if and only if* $\{D_1, D_2, \ldots, D_u\}$ *forms a* $(ku+1, k, k-1; u)$ *near-complete DDF in* G.

Near-complete EDFs can be used to construct a combinatorial object called a *near-resolvable design*. First some background on designs: a (v, b, k, r, λ) balanced incomplete block design (BIBD) is a collection of v points and b blocks; each point is in r blocks and each block contains k points; and every pair of points is contained in exactly λ blocks. A *near parallel class* in a design is a set of blocks that partition all the points except one. A (v, b, k, r, λ) *near-resolvable design* is a BIBD with the property that the blocks can be partitioned into near parallel classes. The *development* of a collection of subsets of a group is the set of all translates of those subsets. The following result shows that the development of a near-complete EDF with constant block size will be a near-resolvable design. This observation is implicit in the comments in Construction II.7.4.5 of [3], and we leave the proof to the reader.

Theorem 2.5 *If* $\{D_1, D_2, \ldots, D_u\}$ *is a* $(ku+1, k, k(u-1); u)$ *near-complete EDF in an abelian group* G, *then the development of the near-complete EDF is a* $(ku+1, (ku+1)u, k, ku, k-1)$ *near-resolvable design.*

The next sections contain new constructions and examples of near-complete EDFs. The final section introduces two other variations, near-complete external partial DFs (EPDFs) and near-complete external divisible DFs (EDDFs), together with examples for each of those.

3 Constructions via partial difference sets

All of the examples from Theorem 2.1 are near-complete EDFs in elementary abelian groups. The following are two new examples of near-complete EDFs in non elementary abelian groups.

Example 3.1 Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ and choose the three subsets

$$\begin{aligned} D_1 &= \{(1, 2), (2, 1), (2, 2), (2, 3), (3, 2)\};\\ D_2 &= \{(0, 1), (0, 3), (1, 3), (2, 0), (3, 1)\};\\ D_3 &= \{(0, 2), (1, 0), (1, 1), (3, 0), (3, 3)\}.\end{aligned}$$

An easy check demonstrates that these form a (16, 5, 10; 3) near-complete EDF. We observe that, for each i, $\{D_i \cup (0, 0)\}$ is a (16, 6, 2) DS in $\mathbb{Z}_4 \times \mathbb{Z}_4$.

Example 3.2 Let $G = \mathbb{Z}_8 \times \mathbb{Z}_8$ and choose the three subsets

$$\begin{aligned} D_1 = \{&(0, 1), (0, 3), (0, 5), (0, 7), (2, 1), (6, 3), (2, 5), (6, 7), (1, 4), (2, 0), (3, 4),\\ &(5, 4), (6, 0), (7, 4), (1, 5), (2, 2), (3, 7), (5, 1), (6, 6), (7, 3), (0, 4)\};\\ D_2 = \{&(1, 0), (3, 0), (5, 0), (7, 0), (1, 2), (3, 6), (5, 2), (7, 6), (4, 1), (0, 2), (4, 3),\\ &(4, 5), (0, 6), (4, 7), (1, 7), (2, 6), (3, 5), (5, 3), (6, 2), (7, 1), (4, 0)\};\\ D_3 = \{&(1, 1), (3, 3), (5, 5), (7, 7), (1, 3), (3, 1), (5, 7), (7, 5), (6, 1), (4, 2), (2, 3),\\ &(6, 5), (4, 6), (2, 7), (1, 6), (2, 4), (3, 2), (5, 6), (6, 4), (7, 2), (4, 4)\}.\end{aligned}$$

An easy check demonstrates that these form a (64, 21, 42; 3) near-complete EDF in G, This example can be found (with a different motivation) in [16].

These examples suggest a general approach of partitioning the nonidentity elements of a group into partial DSs (PDSs) where each PDS has the same number of elements.

Definition 3.3 A k-element subset D of an additive group G of order v is a (v, k, λ, μ)-PDS if the multiset $\{d_1 - d_2 | d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of D exactly λ times and each nonidentity element of $G \backslash D$ exactly μ times.

We often use the group ring to verify that a subset is a PDS (this necessitates our temporarily switching to multiplicative notation). If we allow the usual abuse of notation by writing D both as a subset of G and also $D = \sum_{d \in D} d$ in the group ring $\mathbb{Z}[G]$ (and we also have $G = \sum_{g \in G} g$, $D^{(-1)} = \sum_{d \in D} d^{-1}$, and 1_G as the identity of the group), then we get the following equation for a PDS D.

$$DD^{(-1)} = k1_G + \lambda D + \mu (G - D - 1_G).$$

Similarly, in this language, the group ring equation for a $(v, k, \lambda; u)$-EDF $\{D_1, D_2, \ldots, D_u\}$ is given by

$$\sum_{i=1}^{u} \sum_{j \neq i} D_i D_j^{(-1)} = \lambda (G - 1_G).$$

Theorem 3.4 *Suppose $D_1, D_2, \ldots, D_u$ are (v, k, λ, μ) PDSs that partition the nonidentity elements of a group G. Then $\{D_1, D_2, \ldots, D_u\}$ is a $(ku+1, k, ku-1-\lambda-(u-1)\mu; u)$ near-complete EDF in G.*

Proof From the comments after Definition 3.3, we have, for $1 \leq i \leq u$,

$$D_i D_i^{(-1)} = k1_G + \lambda D_i + \mu (G - D_i - 1_G).$$

Using the fact that the D_i partition the nonidentity element of the group, we get

$$\begin{aligned}\sum_{i=1}^{u} D_i D_i^{(-1)} &= \sum_{i=1}^{u} (k1_G + \lambda D_i + \mu (G - D_i - 1_G)) \\ &= ku1_G + (\lambda - \mu)\left(\sum_{i=1}^{u} D_i\right) + \mu \sum_{i=1}^{u} (G - 1_G) \\ &= ku1_G + (\lambda - \mu + u\mu)(G - 1_G). \end{aligned} \tag{1}$$

Thus, $\{D_1, D_2, \ldots, D_u\}$ is a near-complete DDF and hence is also a near-complete EDF by Theorem 2.4. □

Both Examples 3.1 and 3.2 are covered by Theorem 3.4. Partitioning a group with PDSs is a common technique used to construct Association Schemes [16], so examples from Association Schemes provide a source for near-complete EDFs.

An interesting example of new near-complete EDFs comes from Paley PDSs, which have parameters $\left(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4}\right)$ for $v = 1 \bmod 4$. The original Paley construction uses the squares and non squares in the field $GF(q)$ for q a prime power, so those examples fall under Theorem 2.1. Paley PDSs have been constructed for groups of the form $G = (\mathbb{Z}_{p^{r_1}})^2 \times (\mathbb{Z}_{p^{r_2}})^2 \times \cdots \times (\mathbb{Z}_{p^{r_s}})^2$ for $r_1, r_2, \ldots, r_s \in \mathbb{Z}^+$ [8], so those give examples of near-complete EDFs in non-elementary abelian p-groups.

Even more interesting are the constructions of Paley PDSs in [15] for groups of the form $\mathbb{Z}_3^2 \times \mathbb{Z}_p^{4s}$ for p any odd prime. The group is not a p-group and hence any near-complete EDF constructed in this group will have a different set of parameters than any near-complete EDF that exists in a finite field. We focus our corollary on this case to emphasize the fact that these examples will definitely produce new near resolvable designs.

Corollary 3.5 *For p an odd prime, the group $G = \mathbb{Z}_3^2 \times \mathbb{Z}_p^{4s}$ contains a $\left(9p^{4s}, \frac{9p^{4s}-1}{2}, \frac{9p^{4s}-1}{2}; 2\right)$ near-complete EDF. Therefore for all odd primes p there is a $\left(9p^{4s}, 18p^{4s}, \frac{9p^{4s}-1}{2}, 9p^{4s}-1, \frac{9p^{4s}-3}{2}\right)$-near-resolvable design.*

Proof The first claim comes from [15] and the second claim comes from Theorem 2.5. □

4 Construction via Galois rings

A different construction comes from using Galois rings to generalize Theorem 2.1. For background on Galois rings see [6]. For a given prime p, we define $GR(p^2, r) = \mathbb{Z}_{p^2}[x]/\langle \phi(x) \rangle$ for $\phi(x)$ a basic primitive polynomial of degree r (a degree r polynomial that divides $x^{p^r} - 1$, similar to primitive polynomials for field extensions). The ring $GR(p^2, r)$ is a finite local ring with a unique maximal ideal $pGR(p^2, r)$. The multiplicative group of $GR(p^2, r)$ is isomorphic to $\mathbb{Z}_{p^r-1} \times \mathbb{Z}_p^r$ and consists of all of the elements of the ring not in the maximal ideal. If ξ is an element of multiplicative order $p^r - 1$, then the set $\mathcal{T} = \{0, 1, \xi, \xi^2, \dots, \xi^{p^r-2}\}$ is a complete set of (additive) coset representatives for the maximal ideal: this set is called the *Teichmuller system* for the ring. Every element x of the ring has a unique p-adic representation $x = t + pt'$, where $t, t' \in \mathcal{T}$, and if $t \neq 0$ then $x = t(1 + pt^{-1}t')$. If $K = \langle\xi\rangle$, then K has $\frac{p^{2r}-p^r}{p^r-1} = p^r$ (multiplicative) cosets $D_t = (1 + pt)K$ $(t \in \mathcal{T})$, and we include $D_p = pK = pGR(p^2, r)\backslash\{0\}$ as a coset even though it is not part of the multiplicative group of the Galois ring. The following theorem shows that this collection of subsets will be a near-complete EDF.

Theorem 4.1 *Let $K = \langle\xi\rangle \subset GR(p^2, r)$. The multiplicative cosets D_t $(t \in \mathcal{T})$ and D_p described above form a $(p^{2r}, p^r - 1, p^r(p^r - 1); p^r + 1)$ near-complete EDF in the additive group of $GR(p^2, r)$.*

Proof The proof is analogous to the proof for Theorem 2.1. For invertible elements x and y where $y = zx$ for z an invertible element, if $x = g - g'$ for $g \in D_t$, $g' \in D_{t'}$ with $t, t' \in \mathcal{T}$, then $y = zg - zg'$ for zg and zg' invertible elements coming from different invertible cosets. Thus, x and y will share the same number of solutions coming from pairs of distinct invertible cosets. There are $\frac{p^{2r}-p^r}{|K|}\left(\frac{p^{2r}-p^r}{|K|} - 1\right)$ ways to choose D_i and D_j with invertible elements and each of these choices will produce $|K|^2$ differences. Out of these $|K|^2$ differences, exactly $|K|$ will be elements of the maximal ideal: every difference of elements of the form $x = (1 + pt)(t'') \in D_t$, $y = (1 + pt')(t'') \in D_{t'}$ will satisfy $x - y = p(t - t')t'' \in pGR(p^2, r)$. So each invertible element will have

$$\frac{\frac{p^{2r}-p^r}{|K|}\left(\frac{p^{2r}-p^r}{|K|} - 1\right)(|K|^2 - |K|)}{p^{2r} - p^r} = \left(p^r - 1\right)\left(p^r - 2\right),$$

differences of this form.

We next consider differences $\pm(g - pg')$ where $g \in D_t$ and $pg' \in D_p$. If $x = \pm(g - pg')$, then $y = \pm(zg - p(zg'))$, so we still have the same number of differences for every invertible element where the differences have one element invertible and the other element from D_p. We can choose any of the $\frac{p^{2r}-p^r}{p^r-1} = p^r$ cosets D_t to combine with an element from D_p. The total number of differences is therefore $2p^r(p^r - 1)^2$. Each invertible element will have

$$\frac{2p^r(p^r - 1)^2}{p^{2r} - p^r} = 2\left(p^r - 1\right),$$

differences of this form. When combined with the first computation we see that each invertible element will have a total of

$$\left(p^r - 1\right)\left(p^r - 2\right) + 2\left(p^r - 1\right) = p^r\left(p^r - 1\right),$$

differences as claimed.

Finally we handle the case of noninvertible elements. We first observe that each noninvertible element will have the same number of differences by a similar argument to the previous ones: if x and y are noninvertible, then there is an invertible z so that $y = zx$. If $x = g - g'$ for g, g' in different cosets of K, then $y = zg - zg'$ for zg, zg' in different cosets of K and hence x and y have the same number of differences from distinct cosets of K. There are a total of $(p^r+1)(p^r)(p^r-1)^2$ differences between the cosets, and $(p^{2r}-p^r)p^r(p^r-1)$ of those differences are invertible leaving

$$\left(p^r+1\right)\left(p^r\right)\left(p^r-1\right)^2-\left(p^{2r}-p^r\right)p^r\left(p^r-1\right)=p^r\left(p^r-1\right)^2,$$

noninvertible differences. Since each of the noninvertible elements has an equal number of differences, we have

$$\frac{p^r(p^r-1)^2}{p^r-1}=p^r\left(p^r-1\right),$$

differences per noninvertible element. □

Since the field $GF(p^{2r})$ has a multiplicative subgroup of order p^r-1, the near-complete EDFs in Theorem 4.1 have the same parameters as the near-complete EDFs coming from Theorem 2.1 for a subgroup of order p^r-1. It is not known in general if the associated near-resolvable designs are nonisomorphic.

A completely analogous proof leads to the following similar result.

Corollary 4.2 *Let $K=\langle\xi\rangle\subset GR(p^3,r)$. The multiplicative cosets $D_{t,t'}:=(1+pt+p^2t')K(t,\ t'\in\mathcal{T})$; $D_{t''}:=(p+p^2t'')K(t''\in\mathcal{T})$; and $D_{p^2}:=p^2K$ form a $(p^{3r},\ p^r-1,\ p^r(p^{2r}-1);\ p^{2r}+p^r+1)$ near-complete EDF in the additive group of $GR(p^3,r)$.*

We conjecture that there will be a $(p^{sr},\ p^r-1,\ p^r(p^{(s-1)r}-1);\ p^{(s-1)r}+\cdots+p^r+1)$ near-complete EDF in the additive group of $GR(p^s,r)$.

5 Some further variations and examples

We present two variations on the definition of EDFs, both of which are motivated by various types of DSs. The first is a modification of a PDS which was used in the last section. We note here that the variations presented in this section allow the possibility that the subset sizes may not be constant.

Definition 5.1 Let G be a finite group of order v. Let $D_1,D_2,\ldots,D_u$ be subsets of G that partition the nonidentity elements of G, let $k_i=|D_i|$ for each $1\le i\le u$, and let $\gamma\in\{1,\ldots,u-1\}$. We say that $\{D_1,\ D_2,\ldots,D_u\}$ is a $(v,\ \{k_1,k_2,\ldots,k_u\},\ \lambda,\ \mu;\ u,\ \gamma)$ near-complete EPDF in G relative to $\cup_{i=1}^{\gamma}D_i$ if every nonidentity element $x\in\cup_{i=1}^{\gamma}D_i$ has λ representations $x=g-g'$ with $g\in D_i,\ g'\in D_j(i\ne j)$ and every nonidentity element $x\in(G\setminus\cup_{i=1}^{\gamma}D_i)\}$ has μ such representations.

The group ring equation for a $(v,\ \{k_1,k_2,\ldots,k_u\},\ \lambda,\ \mu;\ u,\ \gamma)$ EPDF $\{D_1,\ D_2,\ldots,D_u\}$ is

$$\sum_{i=1}^{u}\sum_{i\ne j}D_iD_j^{(-1)}=\lambda\sum_{i=1}^{\gamma}D_i+\mu\sum_{i=\gamma+1}^{u}D_i.$$

The following theorem provides a general construction for near-complete EPDFs.

Theorem 5.2 *Let G be a group of order v and suppose $D_1,\ D_2,\ldots,D_u$ are a collection of $(v,\ k_i,\ \lambda_i,\ \mu_i)$ PDSs that partition the nonidentity elements of G. Further suppose that* *there exists* $\gamma \in \{1, \ldots, u-1\}$ *such that* $\lambda_i - \mu_i = c_1$ *for* $1 \le i \le \gamma$ *and* $\lambda_i - \mu_i = c_2$ *for* $\gamma + 1 \le i \le u$. *Then* $\{D_1, D_2, \ldots, D_u\}$ *forms a near-complete EPDF with parameters*

$$\left(v,\ \{k_1, k_2, \ldots, k_u\},\ v - 2 - c_1 - \sum_{i=1}^{u} \mu_i,\ v - 2 - c_2 - \sum_{i=1}^{u} \mu_i;\ u, \gamma\right),$$

in G *relative to* $\cup_{i=1}^{\gamma} D_i$.

Remark To ensure construction of a "genuine" near-complete EPDF, we require $c_1 \neq c_2$.

Proof The proof of this is analogous to the proof of Theorem 3.4: the term $(\lambda - \mu)\sum_{i=1}^{u} D_i$ in the original proof must be replaced by

$$\begin{aligned}
\sum_{i=1}^{u} (\lambda_i - \mu_i) D_i &= c_1 \left(\sum_{i=1}^{\gamma} D_i\right) + c_2 \left(\sum_{i=\gamma+1}^{u} D_i\right) \\
&= (c_1 - c_2)\left(\sum_{i=1}^{\gamma} D_i\right) + c_2 \left(\sum_{i=1}^{u} D_i\right) \\
&= (c_1 - c_2)\left(\sum_{i=1}^{\gamma} D_i\right) + c_2 \left(G - 1_G\right).
\end{aligned}$$

This implies that

$$\begin{aligned}
\sum_{i=1}^{u} \sum_{i \neq j} D_i D_j^{(-1)} &= \left(v - 2 - c_2 - \sum_{i=1}^{u} \mu_i\right)(G - 1_G) + (c_2 - c_1)\sum_{i=1}^{\gamma} D_i \\
&= \left(v - 2 - c_2 - \sum_{i=1}^{u} \mu_i\right)\sum_{i=1}^{u} D_i + (c_2 - c_1)\sum_{i=1}^{\gamma} D_i \\
&= \left(v - 2 - c_2 - \sum_{i=1}^{u} \mu_i\right)\sum_{i=\gamma+1}^{u} D_i \\
&\quad + \left(v - 2 - c_2 - \sum_{i=1}^{u} \mu_i\right)\sum_{i=1}^{\gamma} D_i + (c_2 - c_1)\sum_{i=1}^{\gamma} D_i \\
&= \left(v - 2 - c_2 - \sum_{i=1}^{u} \mu_i\right)\sum_{i=\gamma+1}^{u} D_i + \left(v - 2 - c_1 - \sum_{i=1}^{u} \mu_i\right)\sum_{i=1}^{\gamma} D_i.
\end{aligned}$$

□

In order to apply the construction of Theorem 5.2, we must be able to partition a group with PDSs which have the additional property regarding the $\lambda_i - \mu_i$ values. We are aware of two different relevant results, the first of which is from [16] and the second of which is from [4]. We follow each with a corollary recording the parameters of the relevant near-complete EPDFs.

Proposition 5.3 *Let* $G = (\mathbb{Z}_{p^r})^{2t}$. *There exist PDSs* D_i $(1 \le i \le p^t - 1)$ *that form a partition of the nonidentity elements of* G *with* $|D_1| = |D_2| = (x+1)(p^{rt} - 1)$ *and* $|D_i| = x(p^{rt} - 1)$ *for* $i \neq 1, 2$ *and* $x = \sum_{j=0}^{r-1} p^{jt}$. *The parameters of* D_1 *and* D_2 *are*

$$\left(p^{2rt},\ (x+1)\left(p^{rt} - 1\right),\ (x+1)^2 - 3(x+1) + p^{rt},\ (x+1)^2 - (x+1)\right),$$

and for $i \neq 1, 2$, D_i *has parameters*

$$\left(p^{2rt},\ x\left(p^{rt}-1\right),\ x^2-3x+p^{rt},\ x^2-x\right).$$

Corollary 5.4 *If* $x = \sum_{j=0}^{r-1} p^{jt}$, *then the PDSs* $\{D_1, D_2, \ldots, D_{p^t-1}\}$ *in* $G = (\mathbb{Z}_{p^r})^{2t}$ *from Theorem 5.3 form a* $(p^{2rt}, \{k_1, k_2, \ldots, k_{p^t-1}\}, \lambda, \mu;\ p^t-1, 2)$ *near-complete EPDF, relative to* $D_1 \cup D_2$, *where*

$$\begin{aligned}
&u = p^t - 1,\\
&v = p^{2rt},\\
&k_1 = k_2 = (x+1)\left(p^{rt}-1\right),\\
&k_i = x\left(p^{rt}-1\right) \quad (2 < i \leq u)\\
&\lambda = p^{2rt} - 2 - \left(p^{rt} - 2(x+1)\right) - 2\left[(x+1)^2 - 3(x+1) + p^{rt}\right]\\
&\quad - \left(p^t-3\right)\left[x^2 - 3x + p^{rt}\right]\\
&\mu = p^{2rt} - 2 - \left(p^{rt}+4x\right) - 2\left[(x+1)^2 - 3(x+1) + p^{rt}\right] - \left(p^t-3\right)\left[x^2-3x+p^{rt}\right].
\end{aligned}$$

Proposition 5.5 *Let* $r_1, \ldots r_s \in \mathbb{N}$ *with* $r_i \geq 3$, *let* $t \in \mathbb{N}$, *let* $G = (\mathbb{Z}_{2^{r_1}})^2 \times (\mathbb{Z}_{2^{r_2}})^2 \times \cdots \times (\mathbb{Z}_{2^{r_s}})^2 \times (\mathbb{Z}_4)^t$ *and let* $N = 2^{\sum_{i=1}^{s} r_i + t - 1}$. *Then* G *contains subsets* D_1, D_2, *and* D_3 *that partition the nonidentity elements of the group where* D_1 *and* D_2 *are* $(4N^2, 2N^2-N, N^2-N, N^2-N)$ *PDSs and* D_3 *is a* $(4N^2, 2N-1, 2N-2, 0)$ *PDS.*

Corollary 5.6 *With the notation of Proposition 5.5, the PDSs* $\{D_1, D_2, D_3\}$ *in* $G = (\mathbb{Z}_{2^{r_1}})^2 \times (\mathbb{Z}_{2^{r_2}})^2 \times \cdots \times (\mathbb{Z}_{2^{r_s}})^2 \times (\mathbb{Z}_4)^t$ *form a* $(4N^2, \{2N^2-N, 2N^2-N, 2N-1\}, 2N^2, 2N^2-2N+2;\ 3, 2)$ *near-complete EPDF relative to* $D_1 \cup D_2$.

We note that D_1 and D_2 in Proposition 5.5 are actually regular DSs and hence $\lambda_i - \mu_i = 0$; D_3 is a subgroup (with identity element removed) satisfying $\lambda_3 = |D_3| - 1$ and $\mu_3 = 0$.

The second variation of a near-complete EDF is similar to the first in that the number of differences can take two different values, but the "dividing line" between the two different values will be a subgroup rather than a union of the subsets.

Definition 5.7 Let G be a group of order v with normal subgroup N of order m and index n and let $D_1, D_2, \ldots, D_u (|D_i| = k_i, 1 \leq i \leq u)$ be subsets of G that partition the nonidentity elements of G. We say that $\{D_1, D_2, \ldots, D_u\}$ is an $(n, m, \{k_1, k_2, \ldots, k_u\}, \lambda_1, \lambda_2;\ u)$ near-complete EDDF in G relative to N if every nonidentity element $x \in N$ has λ_1 representations $x = g - g'$ where $g \in D_i$, $g' \in D_j (i \neq j)$ and every element $x \in G \backslash N$ has λ_2 representations $x = g - g'$ where $g \in D_i$, $g' \in D_j (i \neq j)$.

One example of a near-complete EDDF comes from a modification of Theorem 4.1. Instead of using the subgroup $K = \langle \xi \rangle \subset GR(p^2, r)$, we use the subgroup $K' = \langle \xi, 1 + p\xi \rangle$. We have $K' \cong \mathbb{Z}_{p^r-1} \times \mathbb{Z}_p$, so there will be p^{r-1} cosets of K' in $GR(p^2, r)^*$. When we also include $pK' = pGR(p^2, r)$ [which only has p elements as opposed to all of the other cosets of K' having $p(p^r-1)$ elements], we get the following.

Theorem 5.8 *Let* $GR(p^2, r) = \mathbb{Z}_{p^2}[\xi]$ *be the Galois ring over* $\mathbb{Z}_{p^2}$ *and let* $K' = \langle \xi, 1 + p\xi \rangle$. *The multiplicative cosets* $D_t := (1+pt)K'$, $t \in \mathcal{T} \cup \{0\}$, *and* $D_p := pK'$ *form a* $(p^{2r}, \{p(p^r-1), \ldots, p(p^r-1), p^r-1\}, p^r(p^r-p), p^{2r}-p^{r+1}+2p-2;\ p^{r-1}+1)$ *near-complete EDDF in the additive group of* $GR(p^2, r)$.

The proof of Theorem 5.8 is analogous to the proof of Theorem 4.1.

Remark 5.9 We leave to future work the question of whether a version of Theorem 5.8 will produce a near-complete EDDF by changing the subgroup to $K_j := \langle \xi, 1 + p\xi, 1 + p\xi^2, \ldots, 1+p\xi^j \rangle$, and also the question of whether we could change the group to $GR(p^s, r)$. Theorem 5.8 was included to give a specific example of a near-complete EDDF.

Acknowledgements We would like to sincerely thank Joe Yucas for his helpful ideas. We would also like to thank the anonymous referees for their careful reading that resulted in significant improvements throughout the paper.

References

1. Beth T., Jungnickel D., Lenz H.: Design Theory. Cambridge University Press, Cambridge (1999).
2. Chang Y., Ding C.: Constructions of external difference families and disjoint difference families. Des. Codes Cryptogr. **40**, 167–185 (2006).
3. Colburn C., Dinitz J.: Handbook of Combinatorial Designs. Chapman Hall, CRC Press, Boca Raton (2007).
4. Davis J.A., Polhill J.: Difference set constructions of DRADs and association schemes. J. Comb. Theory A **117**, 598–605 (2010).
5. Fuji-Hara R., Munemasa A., Tonchev V.: Hyperplane partitions and difference systems of sets. J. Comb. Theory A **113**, 1689–1698 (2006).
6. Hammons A.R., Kumar P.V., Calderbank A.R., Sloane N.J.A., Sole P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inf. Theory **40**, 301–319 (1994).
7. Lander E.: Symmetric Designs: An Algebraic Approach. Cambridge University Press, Cambridge (1983).
8. Leung K.H., Ma S.L.: Partial difference sets with Paley parameters. Bull. Lond. Math. Soc. **27**, 553–564 (1995).
9. Levenshtein V.I.: One method of constructing quasilinear codes providing synchronization in the presence of errors. Probl. Inf. Transm. **7**, 215–222 (1971).
10. Lidl R., Niederreiter H.: Finite Fields. Cambridge University Press, Cambridge (1997).
11. Mullen G., Panario D.: Handbook of Finite Fields. Chapman Hall, CRC Press, Boca Raton (2013).
12. Mutoh Y., Tonchev V.: Difference systems of sets and cyclotomy. Discrete Math. **308**, 2959–2969 (2008).
13. Ng S.-L., Paterson M.B.: Disjoint difference families and their applications. Des. Codes Cryptogr. **78**, 103–127 (2016).
14. Ogata W., Kurosawa K., Stinson D., Saido H.: New combinatorial designs and their applications to authentication codes and secret sharing schemes. Discrete Math. **279**, 383–405 (2004).
15. Polhill J.: Paley type partial difference sets in non p-groups. J. Comb. Theory A **117**, 1027–1036 (2010).
16. Polhill J., Davis J.A., Smith K.: A new product construction for partial difference sets. Des. Codes Cryptogr. **68**, 155–161 (2013).
17. Pott A.: Finite Geometry and Character Theory. Springer Lecture Notes in Mathematics, Berlin (1995).
18. Wilson R.M.: Cyclotomy and difference families in elementary abelian groups. J. Number Theory **4**, 17–42 (1972).